4-4 Researches on Cryptographic Protocols — Standardization and Global Collaborations —

MATSUO Shin'ichiro and OHKUBO Miyako

Cryptography is fundamental technique to achieve security property in information systems. It is not only used alone, also used as combinations of cryptography and communication in communication protocol. Thus, methods for verification of cryptographic protocols and defining security levels become important research. Then they also requested to be done by global collaboration and used through standardization to achieve international consensus. This article describes standardization activities and international collaborations in researches on cryptographic protocols in the second medium-term plan.

Keywords
Cryptographic protocol, Light-weight cryptography, Verification of cryptographic protocol, Standardization, International cooperation

1 Introduction

Cryptography is used for the purpose of protecting information exchanged over the Internet, as well as ensuring the security of various types of information and authenticating network users. Its more practical application includes electronic money and electronic voting, and a lot of research and development is carried out to provide these advanced services.

In most cases, cryptographic algorithms are used as a part of a communication protocol with a combination of encryption, decryption and communication, rather than being used alone. Such a combination is called a cryptographic protocol hereafter in this article. Not only public research organizations like NICT but also universities and private companies have been conducting research on cryptographic protocols, and new cryptographic protocols are proposed and implemented day by day. On the other hand, methods to evaluate the security of such cryptographic protocols have not been fully established in terms of technology and systems. As for technological aspects, although rigorous theoretical research on the security of cryptographic protocols started on a full scale in 2002, the theory has not yet been matured, and there is still no method that can obtain agreement from a third party's objective point of view. Similarly, the evaluation system of the security of cryptographic protocols, such as how and by whom verification should be performed to certify the security, has not been fully examined. In order to secure the above-mentioned objectivities in technology and publicly verifiability in the system, it is necessary for public organizations to play a central role in facilitating examinations, but on the other hand, it is also essential to collaborate with researchers from universities and the private sector who are the major proponents of cryptographic protocols. Needless to say, as cryptography will be thoroughly investigated by the International Organization for Standardization, and the standardized techniques will be widely implemented in the real world, it is important to contribute to international collaborations and standardization activities.

This article describes the external collaborations, standardization activities, and the achievements in research on cryptographic protocols conducted by NICT, a public research organization in Japan, during the second medium-term plan period.

2 Contributions to international standardization on cryptography

2.1 Contribution to ISO standardization

Standardization of cryptography is carried out mainly by ISO/IEC JTC1 SC27 and the IETF. ITU-T does not take the initiative in standardization of cryptography itself, and basically it refers to the cryptography defined by ISO/IEC JTC1. As for the IETF, although a lot of practical cryptographic protocols such as SSL, a typical standard for cryptographic communication on the Web, have been standardized by them, theoretically rigorous security is not fully discussed in their standardization process. On the other hand, in ISO/IEC JTC1's standardization process, standardization is discussed from a theoretical point of view of security, such as academic theses on security evaluations. Therefore, NICT developed the findings of its academic study on cryptographic protocols mainly with ISO/IEC JTC1.

ISO/IEC standardization of cryptography is conducted by JTC1 SC27. There are five working groups (WG) in SC27. Cryptographic algorithms and cryptographic protocols are discussed by WG2, and security evaluation methods are discussed and standardized by WG3.

WG2 started the standardization of anonymous entity authentication protocol (ISO/IEC 20009-2) that authenticates an entity while preserving anonymity in May 2010, where the author serves as a project editor. Anonymous entity authentication protocol is a typical example of basic technology that is applied to applications where anonymity is required, such as electronic voting, and it will be used more widely as cloud computing becomes more popular in the future. At present, the standardization is focused on an entity authentication protocol that utilizes a group signature scheme. In addition, the author serves as head of the WG2 committee in Japan and participates in the international standardization conferences as a representative of Japan.

Moreover, the author serves as an editor in WG3 to implement standardization of Verification of Cryptographic Protocols (ISO/IEC 29128), in terms of security verification of cryptographic protocols that utilize formalized methods described in ***3.2.3***. The standardization will be completed in 2012.

2.2 Contribution to establishing the US standards on cryptography

In 2004, it was announced that there were attack methods on SHA-1, a US-standard hash function that is widely used among the basic technologies of cryptographic protocols[1]. Following this announcement, NIST, an agency to develop technology standards in US, held a global public competition to find a new hash function to replace SHA-1 in 2007.

Although evaluation of e-government recommended ciphers in Japan is carried out by NICT, as the cryptography established by NIST of the US could virtually become the international standard, it not only has a close relation to us but also has a great possibility to be used for the e-government in Japan in the future. However, in that case, if the selection criteria for standard cryptography in the US are different from the standards to be used for Japan's e-government, it will be not only required to perform another evaluation especially in Japan but also it could result in inconsistency in global standards. For this reason, the author took the initiative to suggest consideration of the requirements for Japan's e-government when selecting US standard cryptography for technology evaluation standards.

Specifically, as smart-cards which can make an electronic signature are widely used in Japan's e-government system, we took account of such use case of cryptographic protocols and proposed evaluation methods for hardware, focusing on smart-cards. In this proposal, we used the SASEBO-GII board developed by the National Institute of Advanced Industrial Science and Technology as a common platform for cryptography evaluation, as well as defining a method to implement modules to perform fair and objective evaluation on this board. In addition, based on the common platform and implementation method, we summarized the implementation results of the fourteen algorithms that were shortlisted for the second round of the public competition for hash functions in the US[2].

As described earlier, cryptographic algorithms and cryptographic protocols must be evaluated fairly and objectively from an international viewpoint. For this reason, the evaluation was carried out not only in Japan but also in collaboration with the world top class universities in cryptography for hardware implementation, including Virginia Polytechnic Institute and State University in the US and Université Catholique de Louvain (Catholic University of Louvain) in Belgium. In this joint examination, the author was in charge of the set up of the platform to be evaluated, as well as management of the research project between the three countries. The result was published in international conferences related to hardware implementation, and international journals. It was also published in the SHA-3 Candidate Conference organized by NIST in August 2010, and provided useful suggestions for NIST's evaluation standards for hash functions.

3 External collaboration in cryptographic protocol research

3.1 Joint research on newly proposed attacks

3.1.1 Purpose

Traditionally the research on cryptographic algorithms and cryptographic protocols are based on an assumption that confidential information (i.e. private key) related to encryption is securely managed by service users so that it will not be disclosed to third parties. Therefore, such confidential information is generally stored in a tamper resistant device (a device with a function to make data disappear when someone tries to peek) such as smartcard.

On the other hand, research on tamper resistance of these devices has been developing recently, and it is beginning to be known widely that attackers could obtain a part of the secret information if they take a certain amount of time[3]. Countermeasures against such attacks include increasing the tamper resistance of devices, and adding a function to the cryptographic protocol which can maintain the security even if a part of the confidential information had been disclosed. In this joint research, we took the latter approach. Research on such cryptographic protocols that can maintain the security even after a part of the secret was started to be fully conducted globally since 2008, but security theory that is suitable for the current status of applications and devices has not been established yet. For this reason, we set our focus on a cryptographic protocol that utilizes RFID tags and cell phones and that are vulnerable to attack, and continued our research on security models and studied authentication protocols with provable security. This research was conducted jointly with Columbia University, an internationally recognized authority in the corresponding field.

3.1.2 The result of the joint research

We conducted two research projects for this topic.

One of them was about a authentication protocol for RFID tags, and we conducted research on a cryptographic protocol that maintains the security even if a certain proportion of secrets had been disclosed. When designing such cryptographic protocols, it should be especially considered that only very limited encryption functionalities can be implemented for RFID tags due to the limitations on the size of implementable circuit. Therefore, we constructed a protocol that combines only the algorithms that can be handled as a pseudo-random function such as AES. We also proposed a new security model for this protocol.

The security model defines executable attacks by attackers more rigorously than before. In other words, the following two security requirements were considered for the authentication protocol for RFID.

- Security against forgery of tags: an attack that intercepts communication between RFID tags and RFID readers, in order to forge RFID tags that can perform successful authentication in the next authentication process. If an attack against the confidential information of RFID tags takes too long, it will be detected by the system; therefore, it only takes a part of the information within the allowed time limit.
- Security on privacy protection: an attack to collect previous output from RFID tags to trace the activities of the owner of the RFID tags. As for the attack against privacy, the attackers can spend unlimited time and they can continue their attack even after it was detected by the system, and consequently, they will obtain all the secrets in the RFID tags.

We proposed a security model with all the above features, and presented it in a peer-reviewed international conference, RFIDSec2010[4].

The other topic is to design a protocol that, even if a part of the confidential information (signature key) used for electronic signature has been disclosed, will not lose the security of signature before or after the disclosure. The security of the electronic signature method is also based on the management of private keys, which are often stored in smart-card in e-government systems, however, due to the aforementioned reasons, it is quite possible that a part of these keys could be disclosed. By taking such attacks into consideration, we designed a protocol that divides confidential information and stores it separately into a device that creates electronic signatures and another device called a Helper (i.e. cell phone), so that there is no problem even if the information is disclosed from each device. We also developed a security model, protocol for realization, and mathematical proof of the security for this protocol, and presented them in a peer-reviewed international conference, Intrust2010[5].

3.2 Collaboration for light-weight cryptographic protocol

3.2.1 Light-weight authentication scheme and formal verification scheme

A number of considerations need to be given in order to utilize cryptography in the real world. Some environments where cryptography is used may not satisfy the environment (for proving the security) assumed by the cryptographic algorithm, or others may not have the computing ability assumed by the used media.

In recent years, communication over networks is not necessarily connected via fixed networks in a physically stationary environment such as desktop PCs, but it could be in an environment where the communication media itself, such as a cell phone, changes its physical position, and thus the communication environment changes accordingly. In addition, in many cases the physical form of embedded devices like cell phone is required to be constructed at a low price in a compact size, and such devices physically do not have the same level of computing power as a desktop PC that is traditionally assumed as a media on which cryptographic algorithms are operated. In accordance with this significant change in these years, there is a notable trend in research on implementation of appropriate cryptography, which studies the environment where RFID is used as a communication media.

Moreover, previously the security of cryptographic algorithm has been often presented for each case individually. However, in contrast to this, there is a growing amount of research that aims to automate (to some degree) the proving process of security by utilizing the knowledge of formal verification methods, and eliminating errors that could be caused in the case of individual proving processes.

Following the above trend, collaboration between our group, which had been studying cryptographic protocols to be applied to embedded devices, and The University of Electro-Communications, which has an extensive knowledge on application of formal verification schemes to cryptographic protocols, achieved significant results. The details are outlined below.

3.2.2 Light-weight authentication scheme

Most embedded devices use wireless communication. Here the assumed players are an embedded device used as a communication media and the server that receives the communication from the device. A light-weight authentication scheme can be presented as a protocol performed between two parties, such as an embedded device and a server.

RFID is assumed as a typical example of an embedded device. RFID is roughly categorized into active tags that have their own power source, and passive tags that use external power supplied via the radio channel. Our study assumed passive tags that require more strict physical conditions. Generally (passive) tags are considered to be distributed in large quantities, and it is desirable to produce them at a low cost. Accordingly, the number of gates that can be implemented in a tag will be limited. When considering such limitation on the number of gates and processing time required by the system, the cryptography circuit that can be implemented on an RFID tag will be limited to a kind that is constructed from operations which can be processed by a minute number of gates. Generally, cryptography circuits for asymmetric key schemes need a lot of gates, and require a certain length of processing time. On the other hand, cryptography circuits for symmetric key schemes can be constructed from a relatively small number of gates and the processing speed is fast, therefore, it is suitable when there are physical restrictions.

It is desirable that impersonation resistance, which is a general requirement to satisfy the security of authentication protocols, and consideration for privacy is taken into account for authentication protocol for RFID. This is because it was not necessary to consider these issues in traditional communication between a desktop PC in a fixed location and server, but due to the fact that embedded devices like RFID do not keep the same physical location when communicating and use wireless communication, it is now necessary to consider such issues.

For example, it is desirable to prevent such situations where behavior can be tracked unexpectedly, or an eavesdropper can intercept certain information of the RFID tag or the owner user of the tag, which is not intended for them, from the information that is readable from the communication between the RFID tag and the server. In addition, the desirable secure authentication protocol should be based on assumptions that tags produced at low cost can be obtained easily, and the stored information can be obtained easily by disassembling the tags.

3.2.3 Formal verification scheme

There has been a movement that formal method is utilized for public competitions of cryptographic protocol in recent years. In the revision of the e-Government recommended ciphers list by CRYPTREC[6], a public competition for (mutual) authentication protocol was held, which is currently in process of short listing. One of the requirements of the competition is that it should be possible to verify the security by a formal method. One of the methods to prove security in cryptography is verification by sequences of games. Verification method based on sequences of games sees the situation of attacks as a game between attacker and challenger, and clearly defines the strategies that attackers are allowed to use and the target of the designer of the method. B. Blanchet et al. developed a software tool “CryptoVerif” that verifies security of cryptography by sequences of games. In the verification process of CryptoVerif, attack models and rewriting rules are described by Blanchet’s process calculus[7], and attack models are converted in accordance with the rewriting rules to evaluate whether they can be converted to a model where the security can be realized. Attack models are expressed by combinations of processes that describe oracles which attackers can call. Rewriting rules are described as two processes that satisfy observation equivalence. In a word, observation equivalence is satisfied when two processes can be distinguished by observable values, such as input/output to process, only by a negligible probability. CryptoVerif records input or calculated values of process as an array, and the recorded values can be called and used by other processes. However, it is not allowed to directly specify the index of an array when calling values, and only indirect operation is allowed, such as specifying it by elements that satisfy a criteria.

Introducing a formal verification scheme like CryptoVerif for proving security of the cryptographic protocol will improve the probability of results of verification compared to the traditional individual proving process, and thus it is expected to be an effective method to ensure consistent verification.

3.2.4 Proposed method

We proposed a method that satisfies security requirements which especially need to be considered for two-party communication between an embedded device such as RFID and a server, as described in ***3.2.2***[8] (see Fig. 1).

In addition, we would like to apply the formal verification scheme introduced in ***3.2.3*** to the proposed method in order to prove its security. Specifically, in order to prove the security, we combined the output results of the formal verification scheme with the traditional method where security is proved individually and applied them to suggest that ultimately the proposed protocol is secure.

3.2.5 Future prospects

The proposed protocol can be not only applied to two-party communication between embedded devices and servers, but also applied to authentication between embedded devices. It is often the case that a cryptographic protocol is constructed for an environment that is very different from the actual environment it will be used for. In such cases, the security could not be maintained when the protocol is used in the actual environment. Therefore, it is desirable to assume an environment that has the minimum gap with the reality when constructing a protocol. Especially, when a media such as embedded device is used, the security could be directly affected by physical restrictions. We specifically focused on these points to examine the construction of our proposed method.

In addition, we applied a formal verification scheme in order to prove the security of the proposed method. Such a method is very effective to prove security compared to the traditional method that proves individual protocols, and it can reduce errors during the proving processes and prove the security more efficiently. It is expected that the process of proving security based on a formal verification scheme with use of CryptoVerif can be applied to a cryptographic protocol which is in a similar situation to the proposed protocol.

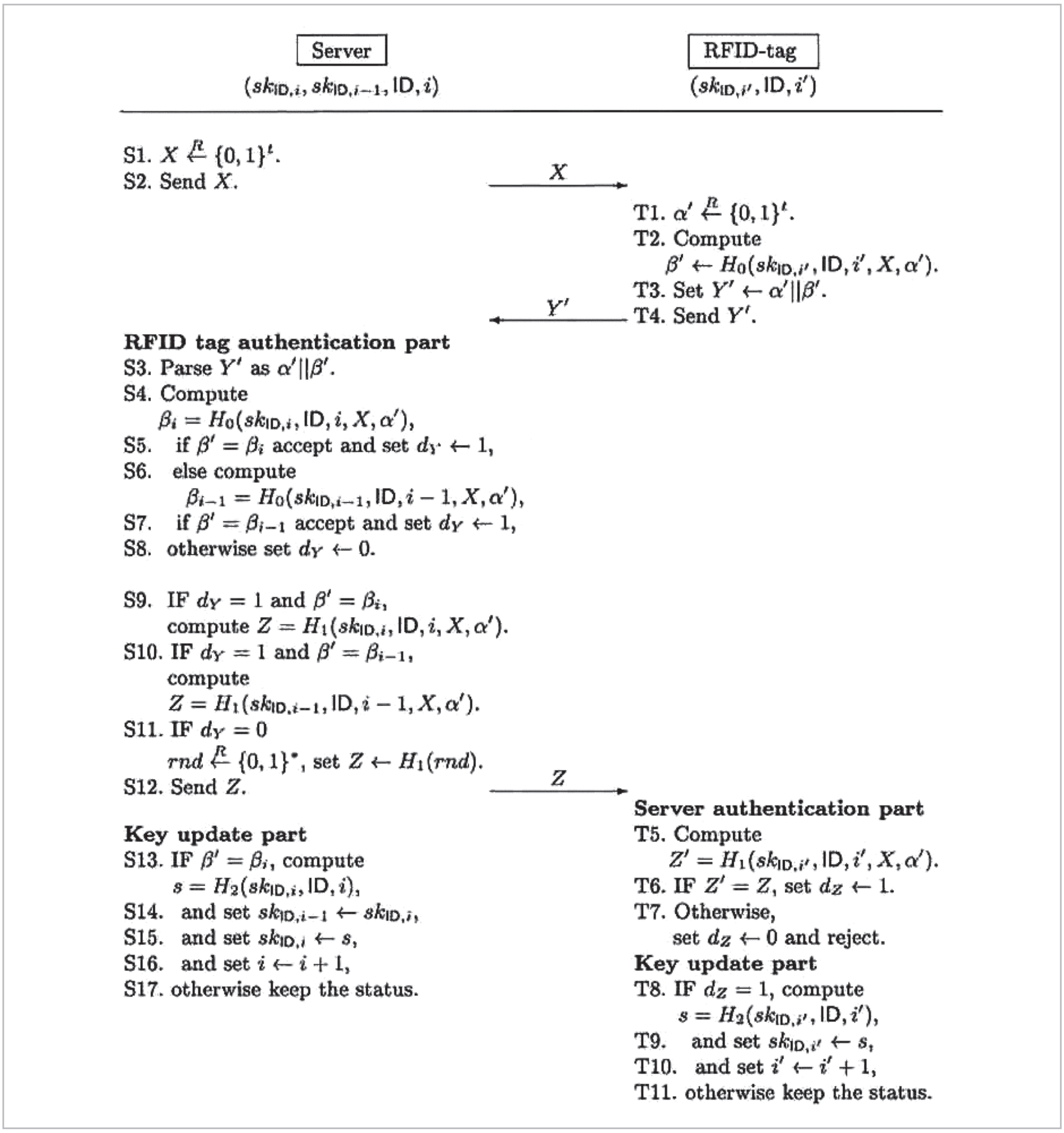
3.3 Collaboration on requirements for cryptographic protocols in realistic systems

3.3.1 Purpose of collaboration

With the advancement of the Internet, research and implementation of various cryptographic protocols have been conducted in order to provide more convenient services through the Internet by secure methods. Examples include electronic money and electronic voting. This research is conducted from various viewpoints, from protocols that satisfy realistic security requirements to ultimate protocols (in terms of security) that can handle every threat to the security assumed in the research.

However, despite the fact that there has been an increase in (academic) research on fully secure cryptographic protocols, there are not many cases where these protocols are implemented and used in the real society. The major cause of this issue is considered to be that although assumed threats are discussed very carefully as a preliminary step for social implementation, optimal solutions that satisfy performance requirements demanded by the society or economically rational operation requirements have not been derived.

While various services based on cryptography and cryptographic protocols have been developed in other countries, Japan, the leading country in research on cryptography in the world, has not managed to apply achievements of research to social implementation: this is a serious issue. For example, the basic infrastructure for cryptographic processing, including encryption and digital signatures, has been developed in Japan, as seen in GPKI or public certification service for individuals; however, the number of applications that utilize this infrastructure remains limited, and the basic resident registration cards which are key have only been issued in limited numbers. In addition, there has been an increase in research on electronic money that can be used as alternative to cash and electronic voting protocols that enable voting on the Internet since the 1990s. However, widely used electronic money services are based on less strict requirements than traditional services that use cash. As for electronic voting, although experiments on voting station type electronic voting systems were conducted in the past, they did not make progress due to information system related issues.



```
Server                                          RFID-tag
$(sk_{\mathsf{ID},i}, sk_{\mathsf{ID},i-1}, \mathsf{ID}, i)$    $(sk_{\mathsf{ID},i'}, \mathsf{ID}, i')$

S1. $X \overset{R}{\leftarrow} \{0,1\}^{\ell}$.
S2. Send $X$.                    $\xrightarrow{X}$
                                                T1. $\alpha' \overset{R}{\leftarrow} \{0,1\}^{\ell}$.
                                                T2. Compute
                                                      $\beta' \leftarrow H_0(sk_{\mathsf{ID},i'}, \mathsf{ID}, i', X, \alpha')$.
                                                T3. Set $Y' \leftarrow \alpha' || \beta'$.
                                 $\xleftarrow{Y'}$     T4. Send $Y'$.
RFID tag authentication part
S3. Parse $Y'$ as $\alpha' || \beta'$.
S4. Compute
      $\beta_i = H_0(sk_{\mathsf{ID},i}, \mathsf{ID}, i, X, \alpha')$,
S5.   if $\beta' = \beta_i$ accept and set $d_{Y'} \leftarrow 1$,
S6.   else compute
          $\beta_{i-1} = H_0(sk_{\mathsf{ID},i-1}, \mathsf{ID}, i-1, X, \alpha')$,
S7.   if $\beta' = \beta_{i-1}$ accept and set $d_Y \leftarrow 1$,
S8.  otherwise set $d_Y \leftarrow 0$.

S9.  IF $d_Y = 1$ and $\beta' = \beta_i$,
     compute $Z = H_1(sk_{\mathsf{ID},i}, \mathsf{ID}, i, X, \alpha')$.
S10. IF $d_Y = 1$ and $\beta' = \beta_{i-1}$,
     compute
     $Z = H_1(sk_{\mathsf{ID},i-1}, \mathsf{ID}, i-1, X, \alpha')$.
S11. IF $d_Y = 0$
     $rnd \overset{R}{\leftarrow} \{0,1\}^*$, set $Z \leftarrow H_1(rnd)$.
S12. Send $Z$.                   $\xrightarrow{Z}$
                                                Server authentication part
                                                T5. Compute
                                                      $Z' = H_1(sk_{\mathsf{ID},i'}, \mathsf{ID}, i', X, \alpha')$.
                                                T6. IF $Z' = Z$, set $d_Z \leftarrow 1$.
                                                T7. Otherwise,
                                                      set $d_Z \leftarrow 0$ and reject.
Key update part                                 Key update part
S13. IF $\beta' = \beta_i$, compute               T8. IF $d_Z = 1$, compute
       $s = H_2(sk_{\mathsf{ID},i}, \mathsf{ID}, i)$,          $s = H_2(sk_{\mathsf{ID},i'}, \mathsf{ID}, i')$,
S14.  and set $sk_{\mathsf{ID},i-1} \leftarrow sk_{\mathsf{ID},i}$,   T9.   and set $sk_{\mathsf{ID},i'} \leftarrow s$,
S15.  and set $sk_{\mathsf{ID},i} \leftarrow s$,            T10.  and set $i' \leftarrow i' + 1$,
S16.  and set $i \leftarrow i + 1$,                 T11. otherwise keep the status.
S17. otherwise keep the status.
```

Fig.1 Construction of light-weight mutual authentication protocol

Thus, there is still a long way to go before Internet voting will be realized.

Therefore, it is necessary to take an approach to derive an “optimum solution” from the viewpoint of applied research on cryptographic protocols and construction of technologies suitable for social implementation. To achieve this, it is important to consider how research on cryptographic protocols can be incorporated into the society. Following this, our study/research aimed to develop guidelines for conducting research on cryptographic protocols for social implementation.

3.3.2 The content of the collaboration

In our research, in order to study cryptographic protocols suitable for social implementation and also to develop any kind of guidelines for finding an “optimum solution” for facilitating social implementation, we researched the best practices in Estonia, the world’s leading country in terms of cryptographic protocols for social implementation, including how cryptographic protocols are discussed to be implemented in the society, how the implementation is accepted by the citizens, what kind of problems have been recognized and how they have been solved.

Although (national) PKI is not used very much in Japan, it is used by almost everybody in Estonia, and especially for Internet voting, Estonia already conducted large scale Internet voting three times in the past. We studied the situation of examination, implementation and problem solving in Estonia, focusing on Internet voting including PKI that provides a platform for it, and compared the situation to the one in Japan to propose what needs to be considered in research on cryptographic protocols in terms of future social implementation in Japan.

The study was conducted through discussions with Professor Ahto Buldas from Tallinn University of Technology, a central figure in research on cryptography/authentication system for e-government in Estonia, and researchers from Cybernetica, a company that designs cryptography/authentication systems for e-government. The research participants visited Estonia and held discussions from December 6 to 19, 2010.

3.3.3 The achievements of the collaboration

First, we conducted research on the ID card/national PKI system, and the electronic voting system in Estonia, and compared them with the PKI and electronic voting system in Japan.

As for the ID card/national PKI system, almost all the nationals in Estonia possess the ID card, although there is no penalty regulation. This is because the ID card is strongly supported not only by the government but also by banks, and as the development environment is released to the public, the hurdle for private enterprises to utilize the ID card is significantly low. In addition, the existence of various applications increases the advantages of using the ID card, which is the key for it gaining in popularity. There have been a growing number of collaborations on applications, and the status of driving license acquisition and ID card information will be linked in 2011, which will make it unnecessary to carry a driving license when carrying an ID card. Thus, there seems to be a strong intention to actively utilize the ID card as the infrastructure for authentication in various scenarios. On the other hand, we found that Estonia had specific circumstances regarding privacy protection. In Japan, if a common ID required for authentication is made open to the public, there are concerns about privacy such as tracking of behavior. In Estonia, however, the nationals did not have strong concerns about privacy protection issues at the time of introduction of the ID card, and that was the reason why the ID card that provided highly convenient services spread rapidly. However, in recent years, some specialists have started pointing out the privacy issues in the use of the ID card, and the government has also started discussing about these issues. At present, although consensus for privacy protection has not been obtained, it is considered that how privacy protection functions can be added to the existing ID card system will be the subject of discussion.

As for electronic voting, the major characteristics of Estonia's case is that they decided to implement Internet voting from the beginning without going through an intermediate solution such as voting station type system. This was related to the fact that they set their objectives for electronic voting with emphasis on not only the reduction of the cost of counting votes but also the idea that increasing the voting rate will raise the quality of democracy. It is also distinctive that, in terms of designing cryptographic protocols, they took an approach that "security measures already available in the existing system should be used as they are, and cryptographic protocols should be applied to only the part where cryptography is newly required" from the viewpoint of social implementation, such as compatibility with the existing systems. Security requirements for Internet voting include "prohibition of voting by a person who does not have voting rights", "prohibition of duplicate voting", "securing anonymity", and "elimination of buying votes". As for elimination of buying votes, they allowed re-voting and significantly reduced the advantages for attackers who attempt to buy votes. As for securing anonymity, instead of adopting a complex system such as Mix-net[9], they introduced operation measures that monitor behaviors of operators including video recording. As a result, a cryptographic process is only required for encryption of voting data, and electronic signatures that are used to confirm the voting rights. As the infrastructure for the ID card was used for the electronic signature, it successfully reduced the cost of constructing an electronic voting system. As a result, thanks to such simple cryptographic protocols, even when counting more than 100,000 votes, the whole process took less than 20 minutes. In addition, the simplicity of the protocol was another major reason why the Estonians accepted the system that heavily depends on the credibility of the centralized server (from a cryptologists' point of view, the grounds for security is based on too many assumptions, and it is not realistic). There are also methods utilizing inspection and video recording to ensure that the system administrators will not take illegal actions (reducing incentives of the system administrators to take illegal actions). Many people suggested that a complex system like Mix-net would be difficult to understand for most ordinary people. Supposedly, if a special protocol such as Mix-net, blind signature, or homomorphic encryption is introduced, the existing infrastructure for the ID card or PKI will not be sufficient to cope with such processes, and extra costs will be required for constructing and operating new systems. It illustrates that it is important to maintain compatibility with the existing infrastructure as much as possible, including a plan to revert to paper voting if any problem occurred.

Based on the aforementioned study/research, we presented a proposal for further research and development on cryptographic protocols that are suitable for social implementation. The key points for such cryptographic protocols include (1) compatibility with the infrastructure that provides existing services, (2) simplicity that users can understand easily, and (3) simplicity that prevents additional costs for constructing a new system. In order to satisfy these points, it is important to utilize the existing infrastructures and operations in terms of the security requirements where the use of cryptographic technology is not required, and adopt such security countermeasures, rather than designing complicated cryptographic protocols. For example, the Internet voting system in Estonia is designed to reduce the incentive of attackers who attempt to buy votes by allowing re-voting, as well as reducing the incentive of operators to commit an inside job by implementing video recording and inspection of operations at every level. As described, the key point is to analyze the incentive of attackers and reduce it by applying various security countermeasures. In the world of cryptographic protocol research, there has been an increase in research on security models based on game theory since around 2002. Most of the existing research has attempted to define security in a rigorous sense within a closed area of cryptographic protocols. However, it is considered that an effective approach for designing cryptographic protocols required for social implementation would be to analyze the risks based on game theory, with input of security requirements for service and attackers' incentives, and then provide solutions based on cryptography for the part where the existing countermeasures are unable to reduce the incentive of attackers.

In 2007, Buldas et al. analyzed the security of Internet voting in Estonia based on a game-theory approach. In designing the basic scheme for Estonia's Internet voting, it seems that the security design was not based on academically systematized game theory at first, however, it can be said that the actual design of the system is (as a result) rational in terms of the aforementioned concept. As for extracting security requirements for cryptographic protocols in the future, we consider that it will become more important to systematize and implement the concept of risk analysis that is based on game theory in designing systems.

4 Summary

This article described researches on cryptographic protocols that are a major technique to secure the security of information communication systems, standardization and our achievements of the collaboration with domestic and international research organizations, as well as describing ISO standardization, contributions toward selecting the US Standards, and the situation of international collaborations to handle more powerful attackers and realistic attacks. International agreement and collaboration is essential to define security standards for cryptographic protocols and to construct secure techniques, and NICT will continue such activities in the future.

Acknowledgements

We would like to extend our gratitude to Professor Kazuo Ohta, Associate Professor Kazuo Sakiyama, and Mr. Yoshikazu Hanatani (The University of Electro-Communications).

References

1 Xiaoyun Wang, Dengguo Feng, Xuejia Lai, and Hongbo Yu, "Collisions for Has Functions MD4, MD5, HAVAL-128 and RIPEMD," IACR Eprint archive 2004/199, Aug. 2004.

2 Shin'ichiro Matsuo, Miroslav Kneoevi¢, Patrick Schaumont, Ingrid Verbauwhede, Akashi Satoh, Kazuo Sakiyama, and Kazuo Ota, "How Can We Conduct Fair and Consistent Hardware Evaluation for SHA-3 Candidate?," NIST SHA-3 Candidates Conference, 2010.

3 Naofumi Honma, Takahumi Aoki, and Akashi Satoh, "Side Channel Attack on Cryptographic Modules and Its Security Evaluation," IEICE Transaction on Fundamentals J93-A(2), pp. 42–51, 2010-02-01.

4 Shin'ichiro Matsuo, Le Trieu Phong, Miyako Ohkubo, and Moti Yung, "Leakage-Resilient RFID Authentication With Forward-Privacy," In Proc of RFID Sec2010, LNCS 6370, pp. 176–188.

5 Le Trieu Phong, Shin Ihiro Matsuo, and Moti Yung, "Leakage Resilient Strong Key-Insulated Signatures in Public Channels," In Proc of INTRUST 2010.

6 CRYPTREC, "Application guidebook for revision of CRYPTREC E-government Recommended Cipher List (2009)," http://www.cryptrec.go.jp/topics/cryptrec20091001 application guide 2009-2.pdf

7 Bruno Blanchet, "A computationally sound mech-anized prover for security protocols," IEEE Transactions on Dependable and Secure Computing, 5(4): 193–207, 2008.

8 Yoshikazu Hanatani, Miyako Ohkubo, Shin'ichiro Matsuo, Kazuo Sakiyama, and Kazuo Ohta, "A Study on Computational Formal Verification for Practical Cryptographic Protocol: The Case of Synchronous RFID Authentication," RLCPS2011.

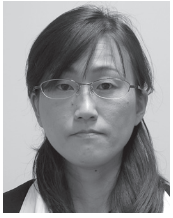
9 M. Abe, “Universally Verifiable Mix-net with Verification Work Independent of the Number of Mix-servers,” In Proc. of Eurocrypt’98, pp. 437–447.

(Accepted June 15, 2011)

MATSUO Shin'ichiro, *Ph.D.*

Director, Security Architecture Laboratory, Network Security Research Institute

Cryptographic Protocol



OHKUBO Miyako, *Ph.D.*

Senior Researcher, Security Architecture Laboratory, Network Security Research Institute

Cryptographic Theory, Cryptographic Protocol